PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 29/06 — A1

(11) International Publication Number: **WO 98/40993**

(43) International Publication Date: 17 September 1998 (17.09.98)

(21) International Application Number: PCT/IL98/00083

(22) International Filing Date: 23 February 1998 (23.02.98)

(30) Priority Data:
120420 10 March 1997 (10.03.97) IL

(71) Applicant *(for all designated States except US)*: SECURITY-7 (SOFTWARE) LTD. [IL/IL]; P.O. Box 107, 20692 Yoqneam (IL).

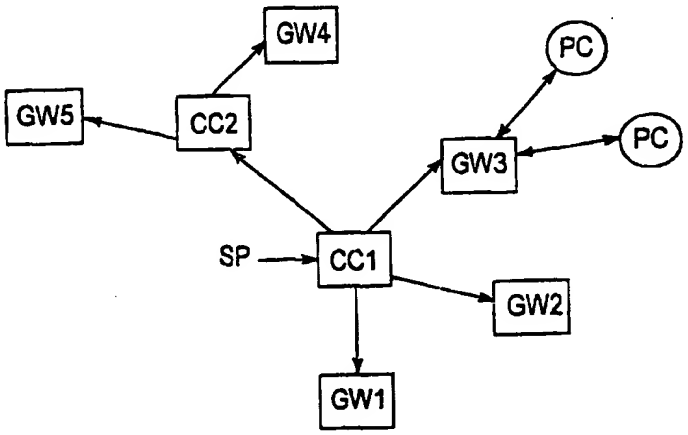
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ELGRESSY, Doron [IL/IL]; 31 Kish Street, 33531 Haifa (IL). JOSPE, Asher [IL/IL]; Nurit Street 39, 42670 Natanya (IL).

(74) Agents: LUZZATTO, Kfir et al.; Luzzatto & Luzzatto, P.O. Box 5352, 84152 Beer-Sheva (IL).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND SYSTEM FOR PREVENTING THE DOWNLOADING AND EXECUTION OF EXECUTABLE OBJECTS



(57) Abstract

A method for selectively preventing the downloading and execution of undesired Executable Objects in a computer, comprising the steps of: (a) providing one or more Control Centers (CC1, CC2), each connected to one or more gateways (GW1... GW5) located between a LAN (PC) and an external computer communication network; (b) providing means coupled to each of said gateways (GW1... GW5), to detect Executable Objects reaching said gateway (GW1... GW5), to analyze the header of each of said Executable Objects, and to determine the resources of the computer (PC) that the Executable Object needs to utilize; (c) providing means coupled to each of said gateways (GW1... GW5), to store a user's Security Policy representing the resources, or combination of resources, that the user allows or does not allow an Executable Object to utilize within its LAN, wherein the Security Policy is received from and/or stored in each of said one or more Control Centers (CC1, CC2); (d) when an Executable Object is detected at the gateway: (GW1... GW5) comparing the resources of the computer (PC) that the Executable Object needs to utilize with the Security Policy.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND SYSTEM FOR PREVENTING THE DOWNLOADING AND EXECUTION OF EXECUTABLE OBJECTS

Field of the Invention

The present invention relates to the security management of computer networks. More particularly, the invention relates to methods and systems for preventing the downloading and execution of undesirable Executable Objects in a workstation of a computer network.

Background of the Invention

The Internet has developed very much both in respect of its contents and of the technology employed, since it began a few years ago. In the early days of the Internet, web sites included text only, and after a while graphics was introduced. As the Internet developed, many compressed standards, such as pictures, voice and video files, were developed and with them programs used to play them (called "players"). Initially, such files were downloaded to the user's workstation only upon his request, and extracted only by the appropriate player, and after a specific order from the user.

When, in the natural course of the development of the World Wide Web the search for a way to show nicer, interactive and animated Web Pages began, Sun Microsystems Inc. developed Java - a language that allows the webmaster to write a program, a list of commands - Network Executables -

that will be downloaded to the user workstation without his knowledge, and executed by his browser at his workstation. The executables are used, e.g., to provide photographic animation and other graphics on the screen of the web surfer. Such executables have some ways approaching the user workstation's resources, which lead to a great security problem. Although some levels of security were defined in the Java language, it was very soon that a huge security hole was found in the language.

Since Java was developed, Microsoft developed ActiveX, which is another Network Executable format, also downloaded into the workstation. ActiveX has also security problems of the same kind.

The Internet has been flooded with "Network Executables" which may be downloaded -- deliberately or without the knowledge of the users -- into workstations within organizations. These codes generally contain harmless functions. Although usually safe, they may not meet the required security policy of the organization.

Once executed, codes may jam the network, cause considerable irreversible damage to the local database, workstations and servers, or result in unauthorized retrieval of information from the servers/workstations. Such elements may appear on Java applets, ActiveX components, DLLs and other object codes, and their use is increasing at an unparalleled pace. The majority of these small programs are downloaded

into the organization unsolicited and uncontrolled. The enterprise has no way of knowing about their existence or execution and there is no system in place for early detection and prevention of the codes from being executed.

The security problem was solved partially by the browser manufactures which allow the user to disable the use of executables. Of course this is not a reasonable solution, since all the electronic commerce and advertising are based on the use of executables. The security problem is much more serious once such an executable can approach the enterprise servers, databases and other workstations.

It is therefore clear that it is highly needed to be able to prevent undesirable Executable Objects from infiltrating the LAN/WAN in which we work and, ultimately, our workstation and server. However, so far the art has failed to provide comprehensive solutions which are safe and quick enough to be practically useful. Systems such as "Firewall" or "Finjan", distributed for use by Internet users, provide only partial solutions and, furthermore, are difficult to install and to update.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a comprehensive method for selectively preventing the downloading and execution of undesired

Executable Objects in a computer, which overcomes the aforesaid drawbacks of prior art systems.

It is another object of the invention to provide such a system which is easy to install and which can be quickly and easily updated.

It is a further object of the invention to provide such a method which can be used with a large number of gateways, LAN's and workstations.

It is yet another object of the invention to provide such a security management system which is independent of the physical infrastructure and network layout.

It is a further object of the invention to provide a system which analyzes the executables "on the fly", and does not hinder the downloading and he operation of harmless executables.

It is yet a further object of the invention to provide a system of the kind described above, which operates as a central security system to which peripheral gateways may be added as needed, to provide a simple, dynamically growing security system.

It is furthermore an object of the invention to provide a central system which permits to define sub-groups of users, each group being subject to a different security policy.

Also encompassed by the invention is a computer system which utilizes the method of the invention.

Other advantages and objects of the invention will become apparent as the description proceeds.

The method for selectively preventing the downloading and execution of undesired Executable Objects in a computer, according to the invention, comprises the steps of:

(a) providing one or more Control Centers, each connected to one or more gateways located between a LAN and an external computer communication network;

(b) providing means coupled to each of said gateways, to detect Executable Objects reaching said gateway, to analyze the header of each of said Executable Objects, and to determine the resources of the computer that the Executable Object needs to utilize;

(c) providing means coupled to each of said gateways, to store a user's Security Policy representing the resources, or combination of resources, that the user allows or does not allow an Executable Object to

utilize within its LAN, wherein the Security Policy is received from and/or stored in each of said one or more Control Centers;

(d) when an Executable Object is detected at the gateway:

1. analyzing the header of said Executable Object;
2. determining the resources of the computer that the Executable Object needs to utilize;
3. comparing the resources of the computer that the Executable Object needs to utilize with the Security Policy and;

(i) if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources allowed for use by the Security Policy, allowing the Executable Object to pass through the gateway and to reach the computer which has initiated its downloading; and

(ii) if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources prohibited for use by the Security Policy, preventing the Executable Object from passing through the gateway, thereby preventing it from reaching the computer which has initiated its downloading.

A Control Center (CC) may be a central control unit, e.g., a PC or other computer, which is connected to a plurality of gateways, and which updates the memory means containing relevant date, e.g., the Security Policy. As will be understood from the description to follow, once the CC is updated, e.g., by the addition of an additional limitation to the Security Policy, all gateways are updated at once. The use of the CC to control the operation of the security elements of the gateways obviates the need (which exists in prior art systems) to update each gateway every time that a change in policy is made.

A LAN (Local Area Network) may be (but is not limited to), e.g., a network of computers located in an office or building. The LAN is typically connected to outside communications networks, such as the World Wide Web, or to more limited LANs, e.g., of a client or supplier, through one or more gateways. The larger the organization, the larger the number of gateways employed, in order to keep communications at a reasonable speed.

Generally speaking, a LAN can also be made of a plurality of smaller LANs, located geographically nearby or far apart, but even if small LANs are found within the same organization, the security requirements may vary from one department to the other, and it may be necessary to keep high security levels, including preventing Executables from migrating from one department to the other, even within the same organization.

The means coupled to each of said gateways, to detect Executable Objects reaching said gateway, to analyze the header of each of said Executable Objects, and to determine the resources of the computer that the Executable Object needs to utilize may be of many different types. Typically, the executable object is "trapped" and analyzed at the gateway by listening on the communication line to the TCP/IP protocol, as well as to the object transfer protocols, such as SMTP, HTTP, FTP, etc. Hooking into the communication line and extracting the contents of the header of the executable object are steps which are understood by the skilled person, and which can be effected by means of conventional programming, and they are therefore not described herein in detail, for the sake of brevity.

Once the header of the Executable Object (EO) has been analyzed, comparing the resources of the computer that the EO needs to utilize with the Security Policy can be easily done, e.g., by comparing them with a look-up table provided to the gateway by the CC, which represents the Security Policy. Comparison can also be carried out against the data stored in the CC, and in such a case specific memory means and comparing means may not be necessary in the gateway. However, speed and performance considerations will often dictate that such operations be carried out at the gateway itself.

The gateway must be installed in each Internet server within the organization. It comprises a small real time database which contains all the relevant operational information for the gateway. The gateway "listens" to the data being transferred between the enterprise and the Internet. It knows when an object is coming into the LAN, it analyzes it and compares it with the Security Policy to decide what action is to be taken.

According to a preferred embodiment of the invention, as stated, if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources allowed for use by the Security Policy, no steps are taken by the system to prevent the Executable Object from passing through the gateway and reaching the computer which has initiated its downloading. However, if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources prohibited for use by the Security Policy, steps will be taken to prevent the Executable Object from passing through the gateway. Such steps may include, e.g., re-routing the executable to a destination outside the gateway, canceling or garbling part of it, so as to make it inoperative, etc.

The invention is not limited to any specific EO. However, according to a preferred embodiment of the invention, the system analyzes EO's including, *inter alia*, Java Applets, Active-X, OCX, Win32 Executables,

DLLs, or the like executable objects. However, as will be apparent to the skilled person, EO's are constantly developed, and the invention is by no means intended to be limited to the use with specific EOs, and the actual nature of the EO is not of critical importance.

According to another preferred embodiment of the invention, the method further comprises the steps of:

(1) when an undesirable Executable Object is detected at a gateway, providing an identifying value therefrom, and notifying all gateways thereof; and

(2) providing memory means and suitable identity verification means, coupled to each gateway, to identify undesirable Executable Objects already analyzed by another gateway, and from preventing it from passing the gateway.

Notifying the other gateways of the existence of undesirable EO's is important inasmuch as this procedure may save considerable time if the EO reaches another gateway, which then does not need to analyze it in detail, to determine the contents of its header, but may decide not to allow its passage by a simpler and quicker procedure, such as checksum.

When more than one Control Centers are provided, Security Policies can be disseminated from one main Control Center to the remaining Control

Centers, and each Control Center, in turn, controls the operation of the gateways connected to it.

According to a preferred embodiment of the invention, each Control Center and each group of gateways is provided with its own individual Security Policy, which may be the same or different from the Security Policy received from the main Control Center. Of course, each subordinate Control Center may add additional limitations to the Security Policy received from the main Control Center, by the addition of resources to the list of those the use of which is not allowed, but according to a preferred embodiment of the invention, it may not remove limitations from the list of limited resources contained in the Security Policy distributed by the main Control Center.

According to a preferred embodiment of the invention, when the system is first installed on the network, the person in charge of security (called hereinafter "CSO" - Chief Security Officer) defines the identity of other Security Officers (SO) who can log-in to the Control Center and make changes in Security Policies. The CSO can define different levels of authority at which the various SOs can operate and make changes to security policies. Other SOs can make changes in the Control Center only if allowed to do so by the CSO, and those changes can affect only clients hierarchically found under their own responsibility. Such changes can only

tighten their client's security policy, with respect to the basic Security Policy, but not loosen it.

Also encompassed by the invention is a computer system comprising one or more LANs, each LAN being connected to an outside computer or computer network through one or more gateways, comprising:

(a) one or more Control Centers, each Control Centers being connected to one or more gateways located between a LAN and an external computer communication network;

(b) means coupled to each of said gateways, to detect Executable Objects reaching said gateway, to analyze the header of each of said Executable Objects, and to determine the resources of the computer that the Executable Object needs to utilize;

(c) means coupled to each of said gateways, to store a user's Security Policy representing the resources, or combination of resources, that the user allows or does not allow an Executable Object to utilize within its LAN, wherein the Security Policy is received from and/or stored in each of said one or more Control Centers;

(d) means, provided at, or coupled to, each gateway:

1. to analyze the header of when an Executable Object which is detected at the gateway;
2. to determine the resources of the computer that the Executable Object needs to utilize;

3. to compare the resources of the computer that the Executable Object needs to utilize with the Security Policy and;

(i) means to allow the Executable Object to pass through the gateway and to reach the computer which has initiated its downloading, if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources allowed for use by the Security Policy; and

(ii) means for preventing the Executable Object from passing through the gateway, thereby preventing it from reaching the computer which has initiated its downloading, if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources prohibited for use by the Security Policy.

The computer system may also comprise, in addition to the means detailed under (d)3 above, also:

(iii) means for alerting the Security Officers that a given type of Executable Object has entered the gateway; and

(iv) means for storing information pertaining to a given Executable Object according to the Security Policy.

Brief Description of the Drawings

In the drawings:

Fig. 1 is a schematic representation of a system according to the invention;

Fig. 2 schematically shows an Executable Object; and

Fig. 3 illustrates the screening function of the gateway operated according to the invention.

Detailed Description of Preferred Embodiments

Looking now at Fig. 1, a possible system is schematically shown, which consists of a main Control Center (CC1), and a subordinate Control Center (CC2). Each CC is connected to a plurality of gateways. The main Control Center (CC1) receives data on the Security Policy (SP) from the operator, and immediately proceeds to update the information in gateways GW1 through GW3, and Control Center CC2 which, in turn, updates GW4 and GW5, including any additional limitations which are set in CC2. Each gateway services a plurality of workstations, typically personal computers. Two such workstations, indicated by PC, are shown in Fig. 1 as being connected to GW3, the remaining workstations not being shown, for the sake of simplicity.

Fig. 2 schematically shows an EO (EO1), which has a header from the analysis of which it can be seen that it needs, in order to function, to use resources x, y, z and w. EO1 is shown in Fig. 3, together with an

additional EO (EO2) and a gateway GW, as seen in the figure. The gateway detects that EO1 needs to utilize resources x and z, which are prohibited according to the Security Policy. Accordingly, EO1 is not allowed to pass the gateway. On the contrary, EO2, which only needs to utilize resources y and w, which are permitted by the Security Policy, is allowed to proceed and to pass the gateway, toward its destination (viz., the workstation which has asked for it).

When an applet enters the LAN it has to declare which workstation within the organization it has to reach. The allowability of the destination is to be checked, since it is possible that a given applet cannot reach one workstation, with a high security level, but can reach another workstation, with a lower security level. Furthermore, the system may change the levels of security on the basis of other considerations, such as the time of the day, the day of the week, etc.

All the above description of preferred embodiments has been provided for the sake of illustration, and is not intended to limit the invention in any way, except as defined by the claims. Many modifications may be effected in the invention. For instance, any number and distribution of Control Centers, Gateways and PCs can be provided, and different Security Policies can be provided by the users. Additionally, a variety of Executable Objects can be monitored, on different infranets and intranets, all without exceeding the scope of the invention.

Claims

1. A method for selectively preventing the downloading and execution of undesired Executable Objects in a computer, comprising the steps of:

(a) providing one or more Control Centers, each connected to one or more gateways located between a LAN and an external computer communication network;

(b) providing means coupled to each of said gateways, to detect Executable Objects reaching said gateway, to analyze the header of each of said Executable Objects, and to determine the resources of the computer that the Executable Object needs to utilize;

(c) providing means coupled to each of said gateways, to store a user's Security Policy representing the resources, or combination of resources, that the user allows or does not allow an Executable Object to utilize within its LAN, wherein the Security Policy is received from and/or stored in each of said one or more Control Centers;

(d) when an Executable Object is detected at the gateway:

1. analyzing the header of said Executable Object;
2. determining the resources of the computer that the Executable Object needs to utilize;
3. comparing the resources of the computer that the Executable Object needs to utilize with the Security Policy and;

(i) if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources allowed for use by the Security Policy, allowing the Executable Object to pass through the gateway and to reach the computer which has initiated its downloading; and

(ii) if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources prohibited for use by the Security Policy, preventing the Executable Object from passing through the gateway, thereby preventing it from reaching the computer which has initiated its downloading.

2. A method according to claim 1, further comprising, in addition to the means of claim 1(d)3:

(iii) means for alerting the Security Officers that a given type of Executable Object has entered the gateway; and

(iv) means for storing information pertaining to a given Executable Object according to the Security Policy.

3. A method according to claim 1, wherein the Executable Object is selected from Java Applets, Active-X, OCX, Win32 Executables, DLLs, or the like executable objects.

4. A method according to any one of claims 1 to 3, further comprising the steps of:

(4) when an undesirable Executable Object is detected at a gateway, providing an identifying value therefrom, and notifying all gateways thereof; and

(5) providing memory means and suitable identity verification means, coupled to each gateway, to identify undesirable Executable Objects already analyzed by another gateway, and from preventing it from passing the gateway.

5. A method according to claim 4, wherein a checksum or the like procedure is carried out on the Executable Object, to generate a substantially unique identification thereof.

6. A method according to claim 1, wherein when more than one Control Centers are provided, Security Policies are disseminated from one main Control Center to the remaining Control Centers, and wherein each Control Center, in turn, controls the operation of the gateways connected to it.

7. A method according to claim 1 or 6, wherein each Control Center and each group of gateways is provided with its own individual Security Policy, which may be the same or different from the Security Policy received from the main Control Center.

8. A method according to claim 7, wherein each subordinate Control Center may add additional limitations to the Security Policy received from the main Control Center, by the addition of resources to the list of those the use of which is not allowed, but it may not remove limitations from the list of limited resources contained in the Security Policy distributed by the main Control Center.

9. A computer system comprising one or more LANs, each LAN being connected to an outside computer or computer network through one or more gateways, comprising:

(a) one or more Control Centers, each Control Centers being connected to one or more gateways located between a LAN and an external computer communication network;

(b) means coupled to each of said gateways, to detect Executable Objects reaching said gateway, to analyze the header of each of said Executable Objects, and to determine the resources of the computer that the Executable Object needs to utilize;

(c) means coupled to each of said gateways, to store a user's Security Policy representing the resources, or combination of resources, that the user allows or does not allow an Executable Object to utilize within its LAN, wherein the Security Policy is received from and/or stored in each of said one or more Control Centers;

(d) means, provided at, or coupled to, each gateway:

1. to analyze the header of when an Executable Object which is detected at the gateway;
2. to determine the resources of the computer that the Executable Object needs to utilize;
3. to compare the resources of the computer that the Executable Object needs to utilize with the Security Policy and;

(i) means to allow the Executable Object to pass through the gateway and to reach the computer which has initiated its downloading, if the resources of the computer that the Executable Object needs to utilize are included in the list of the resources allowed for use by the Security Policy; and

(ii) means for preventing the Executable Object from passing through the gateway, thereby preventing it from reaching the computer which has initiated its downloading, if the resources of the computer that the Executable Object needs to utilize are included

in the list of the resources prohibited for use by the Security Policy.

10. A computer system according to claim 9, further comprising, in addition to the means of claim 9(d)3:

(iii) means for alerting the Security Officers that a given type of Executable Object has entered the gateway; and

(iv) means for storing information pertaining to a given Executable Object according to the Security Policy.

11. A method for selectively preventing the downloading and execution of undesired Executable Objects in a computer, essentially as described and illustrated.

12. A computer system comprising one or more LANs, each LAN being connected to an outside computer or computer network through one or more gateways, essentially as described and illustrated.

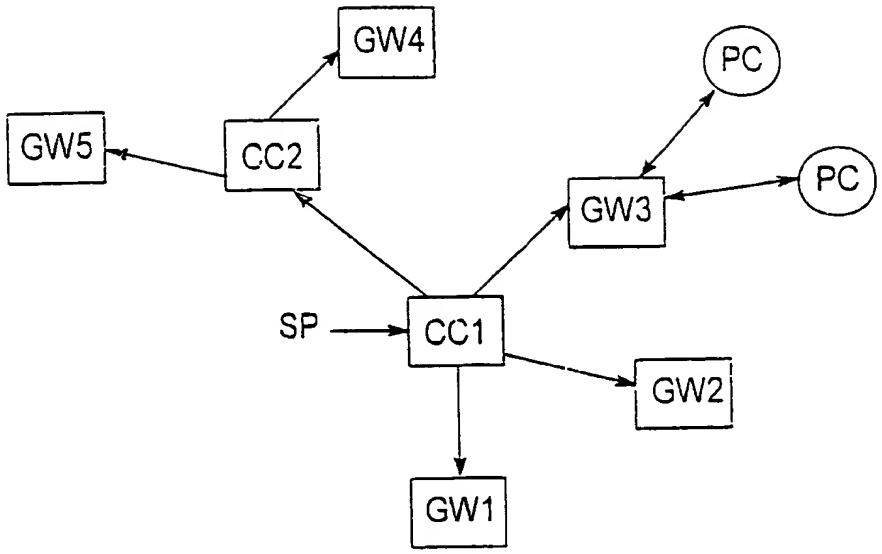


Fig. 1

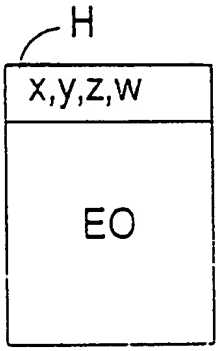


Fig. 2

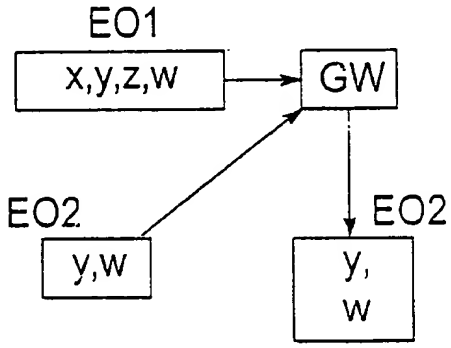


Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IL 98/00083

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L G06F

Documentation searched other than minimumdocumentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SHARON MACHLIS: "Screening for applets" COMPUTERWORLD, vol. 31, no. 6, 10 February 1997, USA, pages 51-52, XP002069848 see page 51, column 1, line 1 - line 29 see page 52, column 1, line 1 - column 2, line 1 ---	1,9
A	DEAN D ET AL: "JAVA SECURITY: FROM HOTJAVA TO NETSCAPE AND BEYOND" PROCEEDINGS OF THE 1996 IEEE SYMPOSIUM ON SECURITY AND PRIVACY, OAKLAND, CA., MAY 6 - 8, 1996, no. SYMP. 17, 6 May 1996, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, pages 190-200, XP000634844 --- -/--	1,9,11

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

' Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of theinternational search	Date of mailing of the international search report
14 July 1998	29/07/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	Adkhis, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IL 98/00083

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 414 833 A (HERSHEY PAUL C ET AL) 9 May 1995 see column 6, line 47 - column 7, line 51 see column 19, line 33 - line 34 see column 27, line 39 - line 69; figure 13 see column 30, line 29 - column 32, line 38 -----	1,9,11, 12

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IL 98/00083

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5414833 A	09-05-1995	NONE	